[Template Data/Personal Information Protection Agreement: Note that this is a sample, template agreement only, and may not be appropriate or sufficient for your particular circumstances. This template is intended for general information and guidance only. Please use thoughtfully, and amend as appropriate. Note that depending on the circumstances (the type of data, location of services/parties, applicable statutes and regulations), additional or different terms may be required to meet applicable statutory/regulatory requirements.]

PERSONAL INFORMATION PROTECTION AGREEMENT

This Personal Information Protection Agreement (the **"Agreement"**) is made as of _____, between [INSERT FULL NAME OF CLIENT/CUSTOMER]("Customer") and INSERT FULL NAME OF SERVICE PROVIDER] (**"Service Provider"**) (each of Customer and Service Provider being a **"Party"**, collectively the **"Parties"**).

WHEREAS Customer and Service Provider have entered into or will be entering into an arrangement involving the provision of[INSERT DESCRIPTION OF THE SERVICES AND OTHER INFORMATION RELEVANT TO THE CONTEXT (e.g. reference to a main agreement under which services are to be performed.)](the **"Services"**);

AND WHEREAS in the course of providing the Services to Customer, Service Provider may receive from Customer and otherwise collect, use, disclose and/or process Personal Information (as defined below) of Customer's employees, clients, customers and/or other individuals;

AND WHEREAS the federal *Personal Information Protection and Electronic Documents Act* (Canada) came into effect on January 1, 2004 with respect to the collection, use and disclosure of personal information of all private sector organizations in the course of commercial activities in Canada. [CONSIDER IF OTHER LEGISLATION IS APPLICABLE]

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged by each of the Parties hereto, the Parties agree as follows:

[If data protection terms are required for incorporation into a broader services agreement, rather than as a free-standing agreement, incorporate the following Sections 1 through 8, with necessary modifications, and consider also an appropriately modified Section 9 to ensure primacy of these data protection provisions over other commercial confidentiality provisions or other terms. Ensure that "Services", "Service Provider", "Customer" and other defined terms used below are modified for consistency with the balance of the broader services agreement. Where appropriate, change references to compliance with "this Agreement" to compliance with "this Article [X]/Section [X]", etc.]

1.

a. **"Applicable Privacy Laws"** means the *Personal Information Protection and Electronic Documents Act*(Canada), as amended or supplemented from time to time, and any other Canadian federal or provincial legislation now in force or that may in the future come into force governing the collection, use, disclosure and protection of personal information **[or personal health information]** in the private sector applicable to either Party or to the Services; **[CONSIDER IF OTHER LEGISLATION SHOULD BE REFERRED TO HERE]** and

Interpretation. For the purposes of this Agreement:

b. **"Personal Information"** means information about an identifiable individual, and includes (without limitation) any information that is "personal information" **[or "personal health information"]** within the meaning of one or more Applicable Privacy Laws. **[CONSIDER IF LEGISLATION HAS A DIFFERENT DEFINITION]**

2. **Personal Information Protection/Safeguards.** To the extent that Customer provides access or transfers to Service Provider any Personal Information in connection with the Services, or to the extent that Service Provider otherwise collects, uses, discloses, stores, processes or otherwise handles Personal Information on behalf of Customer in connection with providing the Services, Service Provider shall:

    a. not use such Personal Information for any purpose other than as necessary for the performance of its obligations with respect to the Services;

    b. not disclose such Personal Information or otherwise permit access to or make such Personal Information available to any person except:

        i. as expressly permitted or instructed by Customer; or

        ii. as required to comply with applicable laws or regulations or a valid court order or other binding requirement of a competent governmental authority, provided that in any such case: (A) Customer is immediately notified in writing of any such requirement (and in any event prior to disclosure of the Personal Information), and (B) Service Provider provides all reasonable assistance to Customer in any attempt by Customer to limit or prevent the disclosure of the Personal Information;

    c. so long as Service Provider remains in possession, custody or control of such Personal Information, use reasonable physical, organizational and technological security measures that are appropriate having regard to the sensitivity of the information to protect such Personal Information against loss, theft and unauthorized access, disclosure, copying, use, modification or disposal; and, without limiting the foregoing, Service Provider shall:

        i. restrict logical and physical access to Personal Information to only those authorized employees and permitted agents and subcontractors that require access to such information to fulfil their job requirements and that are subject to binding obligations of confidentiality and data protection no less stringent than those of this Agreement;

        ii. not print, save, copy or store any Personal Information, whether on removable, mobile or other media, in printed, electronic or optical form or otherwise, except temporarily within a secure location within Service Provider's facilities and only to the extent necessary in connection with providing the Services, and immediately and securely destroy or delete any such temporary copies or saved or stored versions upon conclusion of the activity giving rise to the necessity of saving, copying or storing such Personal Information;

        iii. not move, remove, relocate or transmit any Personal Information from Service Provider's facilities without **[the express consent of Customer] [and/or] [without using appropriately secure encryption technology to protect such information while in transit] [Recent findings and decisions of some Canadian information and privacy commissioners indicate that where the personal information at issue is sensitive, particularly health-related data, some level of encryption is a minimum requirement for meeting an organization's statutory safeguard obligations where transmitting or transporting data electronically (e.g. on laptops, removable media, or over the Internet).]**

iv. **[comply with any additional security measures, processes and procedures set out in Schedule [X]] [Consider adding a schedule of additional security measures and procedures, or referring to existing services schedule that contains security measures or procedures. Depending on the nature of the services, consider whether specifics such as particular encryption technologies, paper shredding technologies, facilities access protocols, or other matters should be addressed.]**

v. **[Where appropriate, consider:][not store, process, communicate, transfer, access or permit or enable access to any Personal Information outside of [Canada/Ontario/Other], or perform any of the Services that involve storing, handling, processing of or access to Personal Information from any location outside of [Canada/Ontario/Other]].**

d. upon termination of the Services or upon request of Customer, whichever comes first, immediately cease all use of and return to Customer or, at the direction of Customer, dispose of, destroy, or render permanently anonymous all such Personal Information, in each case using appropriate physical, organizational and technological security measures to protect such Personal Information against loss, theft and unauthorized access, disclosure, copying, use, or modification consistent with the safeguards and standards set out in Section 2(c) above;

e. immediately inform Customer of any actual or suspected loss, theft or accidental or unauthorized access, disclosure, copying, use, or modification of Personal Information or other breach of Service Provider's obligations in this Section 2;

f. **[If appropriate in the context, consider:]**[subject to any unavailability permitted by service levels agreed to between the Parties in connection with the Services, ensure that Customer at all times has unfettered and unrestricted electronic access to Personal Information stored, processed or handled by Service Provider in connection with the Services.**]**

g. ensure at all times that Personal Information and all data, databases or other records containing Personal Information that are stored, handled or processed for Customer in connection with the Services are kept logically isolated and separate from any information, data, databases or other records stored, handled or processed by Service Provider for itself or for third parties.

3. **Requests, Inquiries and Complaints.** Service Provider shall: (a) immediately refer to Customer any individual who contacts Service Provider requesting access or correction to or with any inquiries or complaints about his or her Personal Information in connection with or otherwise relating to the Services; (b) immediately notify Customer regarding any such request, inquiry or complaint; and (c) provide, in a timely manner, all reasonable co-operation, assistance, information and access to Personal Information in its possession, custody or control as is necessary for Customer to promptly (and, in any event, within any timeframe required by Applicable Privacy Laws) respond to such request, inquiry or complaint.

4. **Audits.** On reasonable notice and during normal business hours, Service Provider shall: (a) permit Customer or its designee to inspect any Personal Information in the custody or possession of Service Provider in connection with the Services and to audit Service Provider's compliance with its obligations described in this Agreement, including, without limitation, the security measures used to protect Personal Information; (b) permit Customer to enter onto Service Provider's premises for such purposes; and (c) otherwise promptly and properly respond to all reasonable inquiries from Customer with respect to Service Provider's handling of Personal Information in connection with the Services or Service Provider's compliance with this Agreement.

5. **Privacy Regulators.** Service Provider shall provide, in a timely manner, all necessary and reasonable information and co-operation to Customer and to any regulatory or other governmental bodies or authorities with jurisdiction or oversight over Applicable Privacy Laws (each, a **"Privacy Regulator"**) in connection with any investigations, audits or inquiries made by any such Privacy Regulator under such legislation. Service Provider acknowledges that Customer may be required to disclose confidential information of Service Provider (including, without limitation, this Agreement and any agreement or other documentation relating to the Services), without Service Provider's consent, to such Privacy Regulators in connection with any investigation, audit or inquiry that pertains to or involves the Services.

6. **Designated Individual.** Service Provider shall designate and identify to Customer an individual to handle all aspects of the Services that relate to the handling of Personal Information.

7. **Subcontracting.** Service Provider shall not subcontract, assign or delegate to any third party its obligations with respect to the collection, use, disclosure, storage, handling or processing of Personal Information in connection with the Services without **[the express written consent of Customer][CONSIDER ALTERNATIVELY: "without prior notification to Customer"]** and without obtaining written contractual commitments of such third party substantially the same as those of this Agreement.

8. **Compliance with Applicable Privacy Laws.** In all cases and without limiting the foregoing, Service Provider shall comply at all times with Applicable Privacy Laws in carrying out the Services.

9. **Amendment and Conflict.** Service Provider and Customer acknowledge and agree that all agreements, contracts or other arrangements (whether written or unwritten) governing the performance of the Services (each, a **"Service Agreement"**) are hereby amended so as to incorporate the terms set out in this Agreement. To the extent of any inconsistency between the terms in this Agreement and those of any Service Agreement as such terms may relate to Personal Information, the terms of this Agreement shall prevail.

10. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario and the federal laws of Canada applicable therein.

IN WITNESS WHEREOF the Parties have executed this Agreement:

[CUSTOMER FULL NAME]	**[SERVICE PROVIDER FULL NAME]**
Per: _____	Per: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____